SOCIAL SECURITY

April 25, 2025

Jeffrey Clark
Acting Administrator
Office of Information and Regulatory Affairs, OMB
Eisenhower Executive Office Building
1650 17th St NW, Washington, DC 20006Washington, D.C. 20503

Dear Acting Administrator Clark,

The Social Security Administration (SSA) is seeking emergency approval from OMB under 5 C.F.R. § 1320.13 of the implementing regulations of the Paperwork Reduction Act (PRA) to implement a new hybrid identity proofing process for respondents to certain information collections. This emergency request covers three changes to existing information collection practices. These changes are:

(1) Require all respondents to use the hybrid identity proofing process (Security Authentication PIN (SAP)) described below any time a respondent seeks to enroll in, update, or cancel their direct deposit information with a technician over the phone; and
(2) Allow individuals who visit a field office, and who under existing practices would be required to provide proof of identity, the ability to authenticate their identity through the use of SAP for direct deposit changes or enrollment only.

The new SAP process will enable members of the public to, via their *my* Social Security account, generate and provide a one-time passcode to augment SSA's current identity verification process, primarily for phone contacts to defend against fraud and misdirection of benefit payments. Emergency approval of this Information Collection Request (ICR) will enable individuals to complete direct deposit associated services over the phone while ensuring fraud protection through verification of the identity of the caller prior to accessing or revising their account.

Background

Our current telephone process requires respondents to use knowledge-based questions to verify their identity. While this process provides some fraud protection and authentication under current NIST specifications, in NIST Special Publication 800-63B[1], *Digital Identity Guidelines*, it still poses a fraud risk, as per GAO-19-288[2], *Federal Agencies Need to Strengthen Online Verification Processes* for respondents who wish to complete tasks for which our other

[1] NIST Special Publication 800-63B
[2] Proving You're You: How Federal Agencies Can Improve Online Verification | U.S. GAO

modalities, including our automated telephone system, in-person interviews, or Internet platforms would request higher levels of identity proofing and authentication. Since direct deposit entails access to the respondents' funds, requires the respondent to divulge or submit banking information, and may affect their benefits payments, we consider the establishment of or revisions to direct deposit account information to be a higher risk task. Direct deposit changes provide an opportunity for attackers to convert beneficiary payments to their own use. Consequently, we consider the establishment of or revisions to direct deposit account information to merit a heightened identity assurance standard.

Currently, we allow for most respondents to make changes to direct deposit information via four different modalities[3]: in-person at a field office; online through *my* Social Security; automated enrollment through the respondents' bank; and through a live telephone call with a technician over the telephone. Prior to April 2025, phone-based direct deposit changes accounted for roughly one-third of all direct deposit change requests, or approximately 35,000 calls per week. For all modalities other than a live telephone call we typically require a heightened level of identity authentication (for example, we require multi-factor authentication through ID.me or Login.gov for our online process prior to allowing respondents access to such sensitive information). Therefore, for fraud protection, we need to implement an equivalent level of identity authentication for our telephone services before SSA technicians can help telephone respondents access or change their sensitive direct deposit information.

The new SAP process for phone-based direct deposit services is an improvement consistent with Executive Order 14249, [4]*Protecting America's Bank Account Against Fraud, Waste, and Abuse*, and recent policy directives.

Overview of Emergency ICR

Security Authentication PIN (SAP) Process for Direct Deposit Changes Over the Phone

Effective in April 2025, SSA will increase the level of identity proofing needed for respondents to make direct deposit changes during phone interactions by no longer allowing respondents to authenticate their identity over the phone using knowledge-based authentication methods when they seek to make changes to their direct deposit information (such as enrolling-in, changing, or cancelling direct deposit). Instead, SSA has created a new hybrid method, called the Security Authentication PIN (SAP) process, which will allow telephone respondents to authenticate their identity during a phone call through their *my* Social Security account. Specifically, SAP will leverage our current Internet identity proofing through Login.gov and ID.me to support telephone interviews for direct deposit requests. We will allow exemptions from the SAP process in extreme dire-need situations (e.g., pre-release, terminal cases, field office banned individuals, etc.).

The hybrid Security Authentication PIN process will require the use of a unique PIN (the SAP) to verify the identity of a respondent who wants to make direct deposit information changes over the phone. This would only apply to situations where the respondents are speaking with an SSA

[3] Note: While Title II recipients can use the online platform for direct deposit requests, Title XVI recipients currently cannot use the online platform for this purpose.

[4] Protecting America's Bank Account Against Fraud, Waste, and Abuse – The White House

employee directly and will require the callers to already possess (or establish) a *my* Social Security account through Login.gov or ID.me (OMB No. 0960-0789). For respondents who call-in to make direct deposit changes the technician would then look up the SSN the caller provided to see if the caller has an associated *my* Social Security account. If the technician finds an associated account in the system for that SSN, the technician will provide a direct vanity link (a custom, user-friendly shortcut URL that redirects to a longer, often more complex destination URL) to the caller through reading it over the phone or by sending the URL to the respondents email or mobile phone using eMailer, which will require the caller to log into their *my* Social Security account to generate a unique, time-limited 8-digit PIN number (the SAP) through the provided link. The technician will then ask the respondent to verbally recount the SAP. If the SAP matches in the system, the technician will then continue with the call and help the respondent with completing the claim, updating bank information, or changing other pertinent payment method requests.

If, however, the technician does not find an associated *my* Social Security account in the system, the technician will instruct the respondent to create a *my* Social Security account, which includes creating a login.gov or ID.me account, and call back once they have completed that task. Once the caller has an account, they will be able to generate the SAP and continue with the call.

Alternatively, the respondent will be able to log into their *my* Social Security Account prior to the call to generate the SAP through a new link to "Generate PIN." Once they have the SAP, they will be able to proceed to call an agency technician to complete their business with SSA over the telephone. The SAP will replace the current knowledge-based questions we ask for authentication under SSA's current credentialing and authentication process (OMB No. 0960-0789), as the respondent will now authenticate through their *my* Social Security account prior to generating the SAP. As discussed in the Supporting Statement A, we will use this process for phone-based direct deposit requests.

In summary, whether the respondent receives the direct link from a technician on the phone or accesses it themselves through their *my* Social Security account, they will ultimately need (1) a *my* Social Security account and (2) a SAP before the technician can help them complete their direct deposit change over the phone. The SAP will allow for multi-factor authentication over live telephone calls, which will alleviate fraud concerns, and allow respondents to do business with the agency securely.

<u>Security Authentication PIN (SAP) Process As an Alternative to Identity Documents for In-Person Authentication for Direct Deposit Requests</u>

For circumstances where a respondent is seeking direct deposit requests in-person at a field office and they are required to provide an acceptable form of identification (e.g., State ID/driver's license, U.S. Passport, etc.), the SAP will provide an alternative option for individuals who do not have the requisite identity document with them at the time.

If the respondent does not have an acceptable form of identification on their person, the technician will ask if the respondent has an online *my* Social Security account. If they do, the technician will provide the respondent with a direct link, either by reading the vanity URL to the respondent or by sending a link via email or text. The respondent can then generate the 8-digit

Security Authentication PIN (SAP) after signing into their account. The PIN will be valid for 30 minutes, after which the respondent can generate a new PIN if required.

Need for Emergency Clearance

To allow for continued security for respondent's personal information, and to ensure SSA is able to accurately verify the callers' identities prior to accessing any SSA number holders' sensitive information, we are implementing this hybrid SAP process for telephone access to the direct deposit services. In this way, we continue to offer maximum flexibility and options to the public while ensuring the security of the public's social security number and benefits payments. We expect this new identity proofing will be a powerful fraud prevention tool.

In accordance with the Paperwork Reduction Act (PRA) and the Office of Management and Budget's (OMB) implementing regulations at 5 C.F.R. § 1320.13, we have found the following: First, per 5 C.F.R. § 1320.13(a)(1), this information is necessary prior to the time periods established under PRA and this information collection is essential to the mission of the agency. As discussed in previous paragraphs, SSA has identified a unique deficiency in how it authenticates the identity of respondents who make direct deposit requests via a phone-based conversation with a technician to the other modalities available to respondents. Per SSA's current data, about 42% of all direct deposit fraud is phone-based. It is incumbent that the agency reduces this risk by ensuring phone-based direct deposit changes have a similar level of identity authentication as is already expected with other modalities. Finally, paying benefits to eligible claimants is essential to the agency's mission. SSA is implementing SAP quickly to reopen a service channel (phone based direct deposit changes) we closed earlier this month due to fraud issues. If we were to conduct the full OMB approval process, we would need to delay the reopening of this service channel, and we would cause undue burden on the public, forcing them to trave l to field offices for direct deposit changes.

Second, per 5 C.F.R. § 1320.13(a)(2), SSA has determined it cannot reasonably comply with normal clearance procedures as public harm is reasonably likely to result if normal procedures are followed. As discussed in the previous paragraph, SSA has identified a unique deficiency in how it authenticates direct deposit requests which are made in a live conversation with a technician over the phone. This notice further discloses to the public these risks. The public may be harmed by, for example, increased attempts at fraudulent changes to beneficiaries' direct deposit information by malicious actors were SSA to attempt to reasonably comply with normal clearance procedure timelines.

Under 5 C.F.R. § 1320.13(d), SSA has received approval to modify its normal Federal Register posting requirements. We are requesting emergency clearance with approval to be granted no later than **04/25/2025**. We published a notice in the Federal Register at 90 FR 16583 to invite the public to submit comments if they wish to do so.

We understand that an emergency PRA approval is effective for only six months. Following the emergency clearance, we may seek full PRA approval for the new hybrid SAP process. During the full approval process, we will also address any public comments we receive on the emergency PRA approval.

We appreciate your collaboration on this important ICR. Please contact me with questions at (410) 907-5418 or at dustin.s.brown@ssa.gov.

Sincerely,

Dustin S. Brown
Deputy Commissioner
for Legislation and Congressional Affairs